SUMMARY OF TESTIMONY BEFORE THE
HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON HEALTH

"Legislative Proposals to Promote Electronic Health Records And a Smarter Health Information System"

Testimony of James C. Pyles, Counsel
American Psychoanalytic Association
March 16, 2006

The entire health delivery system is dependent upon the willingness of individuals to share the most intimate details of their lives with their health care practitioners. A national "interoperable" electronic health information system is unlikely to be accepted by the public and be successful unless it is built upon traditional standards of medical privacy that the public expects and that are part of the standards for the ethical practice of medicine and psychiatry.

The right to medical privacy is widely accepted as the right of the individual to have some control over the disclosure of his or her identifiable health information in most routine situations. This right has been identified throughout the history of medicine and the history of the our nation as essential for quality health care. The right finds its source in the Hippocratic Oath, established standards of medical ethics, the amendments of the Bill of Rights and the 14th Amendment to the U.S. Constitution, the physician-patient and psychotherapist-patient privilege, and the statutory and common law of every state.

The right to privacy and consent was not recognized and protected in the HIPAA Amended Privacy Rule implemented on April 14, 2003. However, the Department of Health and Human Services explained in issuing the rule that it was only intended as a "floor" of privacy protections and that it was not intended to preempt more protective state privacy laws nor override established standards of medical ethics.

The public wants strong health information privacy protections preserved and fears that a national electronic health information system will eliminate the right to privacy and consent. Any electronic health information legislation should be built on the privacy principles reflected in standards of medical ethics, the law of medical privilege, constitutional common law, and state laws. There should be no preemption of state laws unless and until Congress enacts strong national health information privacy standards and principles.

James C. Pyles
Powers, Pyles, Sutter, & Verville, P.C.
1875 Eye Street, NW
Washington, D.C. 20006
(202) 466-6550
jim.pyles@ppsv.com

House Committee on Energy and Commerce

Witness Disclosure Requirement - "Truth In Testimony"
Required by House Rule XI, Clause 2(g)

Your Name: James C. Pyles

1. Are you testifying on behalf of a Federal, State, or Local Government entity?	**Yes**	**(No)**
2. Are you testifying on behalf of an entity other than a Government entity?	**(Yes)**	**No**

3. Please list any federal grants or contracts (including subgrants or subcontracts) which you have received since October 1, 1999: None

4. Other than yourself, please list what entity or entities you are representing:
American Psychoanalytic Association

5. If your answer to question number 2 is yes, please list any offices or elected positions held or briefly describe your representational capacity with the entities disclosed in question number 4: Counsel

6. If your answer to question number 2 is yes, do any of the entities disclosed in question number 4 have parent organizations, subsidiaries, or partnerships to the entities for whom you are not representing?	**Yes**	**(No)**

7. If the answer to question number 2 is yes, please list any federal grants or contracts (including subgrants or subcontracts) which were received by the entities listed under question 4 since October 1, 1999, which exceed 10% of the entities revenue in the year received, including the source and amount of each grant or contract to be listed: None

Signature: James C Pyles **Date:** 3/14/06

WILL A NATIONAL "INTEROPERABLE" HEALTH INFORMATION SYSTEM PRESERVE OR ELIMINATE THE PATIENT'S RIGHT TO HEALTH INFORMATION PRIVACY?

Health Subcommittee of House Committee on
Energy and Commerce
March 16, 2006

James C. Pyles
Counsel
American Psychoanalytic Association

I. **Fundamental question presented by health IT bills**—Will Congress **compel Americans** to disclose all of their most sensitive health information about themselves and their families to and from a national "interoperable" health information system **without meaningful, informed patient consent, against their will and without adequate enforcement against unauthorized uses and disclosures?**

A. Without a right to **privacy**, there can be no **liberty**, and Americans will not have access to **quality health care**.

B. If Americans' privacy for their **inner-most thoughts** and their **genetic make-up** is not protected, they will not seek treatment or support the use of electronic health records.

II. **What does meaningful consent and privacy mean?**

A. HHS--The ability of individuals "to **determine for themselves** when, how, and to what extent information about them is communicated." [1]

B. Courts—**"control over knowledge about one's self**...one of the most **fundamental and cherished** rights of American citizenship, falling within the right

[1] 65 Fed. Reg. at 82,465.

characterized by Justice Brandeis as 'the right to be let alone'." [2]

III. Why is the right to health information privacy important?

A. HHS Findings--

i. "In short, the **entire health care system** is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers." [3]

ii. "While privacy is one of the key values on which our society is built, it is more than an end in itself. It is also necessary for the **effective delivery of health care**, both to individuals and to populations." [4]

iii. "Unless public fears are allayed, we will be **unable to obtain the full benefits of electronic technologies.** The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this **primarily financially-driven expansion** in the use of electronic data." [5]

IV. Sources of the nationally and locally recognized right to meaningful consent and health information privacy.

A. The **Hippocratic Oath** dating from the 5th Century B.C. which is administered to graduates by 98% of the medical schools in the U.S. and Canada. [6]

---

[2] U.S. v. Westinghouse, 638 F.2d 570, 576, 577, n. 5 (3rd Cir. 1980).
[3] 65 Fed. Reg. at 82,467.
[4] 65 Fed. Reg. at 82,467.
[5] 65 Fed. Reg. at 82,466..
[6] "The Use of the Hippocratic Oath", R. Orr, M.D. and N. Pang, M.D.

B. **Established standards for the ethical practice of medicine** adopted by every segment of the medical profession which state that

1. "The physician **should not reveal confidential communications or information** without the express consent of the patient, unless otherwise required to do so by law." [7]

C. The **Fourteenth, Fifth, Fourth, and First Amendments to the U.S. Constitution**—this is the **"informational"**, rather than the "decisional" branch, of the right to privacy which the Supreme Court has consistently found provides that an individual's personal health information may not be disclosed without his or her consent unless there is a **"compelling" governmental interest,** and even then the government must use the **"least intrusive alternative".** [8]

1. Consent must also be **voluntary and informed.** [9]

D. **The physician-patient privilege** recognized in most states. [10]

E. **The psychotherapist-patient privilege**—recognized in all 50 states and the District of Columbia and in Federal common law. [11]

F. **Tort laws or statutory laws** in all 50 states recognize a right to privacy. Some states, like **Tennessee and California** have an explicit right to privacy in their State Constitutions. [12]

---

[7] See Principles of Medical Ethics of the American Medical Association and many other medical associations and societies in Tab 1.

[8] Ferguson v. City of Charleston, 532 U.S. 67; Whalen v. Roe, 429 U.S. 589 (1977); Sell v. United States, 539 U.S. 166, 181 (2003); Tucson Woman's Clinic v. Eden, 371 F. 3d 1173 (9th Cir. 2004).

[9] Ferguson v. City of Charleston, 308 F.3d 380, 399 (4th Cir. 2002).

[10] Northwestern Mem. Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004).

[11] See Jaffee v. Redmond, 518 U.S. 1 (1996).

[12] 65 Fed. Reg. at 82,464.

G. **State laws, in Georgia and Ohio**, for example, provide privacy protections for health information held by health care facilities, physicians, pharmacists, and long term care facilities, as well as special protections for **alcohol and drug abuse, genetic testing, HIV/AIDS, mental health, sexually transmitted disease, cancer and birth defect information** as well as provide a **private right of action** for violations. [13]

H. Health information **currently has privacy protection** under **most state laws** that is not provided by the HIPAA Privacy Rule

   i. Mental health information

   ii. Genetic testing information

   iii. Cancer diagnosis and treatment information

   iv. HIV/AIDS testing and treatment information

   v. Drug and alcohol abuse diagnosis and treatment information

   vi. Birth defect information [14]

   vii. At the state level, specific patient authorization is often required before this type of sensitive health information can be disclosed.

I. **Other privacy protections** recognized under state law.

   i. Privacy breach **notification** —29 states now have these laws

   ii. **Private right of action** [15]

---

[13] See list of Georgia and Ohio health information privacy laws summarized in Tab 2.
[14] See summaries of these laws for the states of Georgia and Ohio.

iii. **Physician-patient privilege** statutes and common law—recognized in most states [16]

iv. **Psychotherapist-patient privilege** laws—recognized in all 50 states and the District of Columbia [17]

v. The right to privacy and consent under an **implied contract** between physicians and patients [18]

V. The right to privacy under HIPAA

A. HIPAA Privacy **Rule**— provides **"regulatory permission" for all covered entities** and business associates to use and disclose identifiable health information for all routine purposes (**treatment, payment and health care operations**): [19]

i. without **notice**

ii. without **consent**

iii. over the individual's **objection**

iv. even if the individual **pays privately**

v. even information **prior to the compliance date** [20]

B. **Treatment, payment, and health care operations** include nearly 100 uses that **broadly eliminate** the individual's right to health information privacy. [21] In short,

---

[15] Both Georgia and Ohio permit a private right of action for breaches of health information privacy under state law. Tab 2.
[16] Northwestern Mem. Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004).
[17] Jaffee v. Redmond, 518 U.S. 1 (1996).
[18] Givens v. Millikin, 75 S.W. 3d 383 (Tenn. 2002).
[19] 67 Fed. Reg. at 53,211 Tab 3.
[20] 45 C.F.R. 164.506(a) (amended) Tab 3.
[21] See list of uses included in treatment, payment and health care operations at Tab 4.

patients have no meaningful right to control their own health information.

C. **HHS response to comments** that the privacy rule **violates state law and medical ethics**

1. The HIPAA Privacy Rule is **only a "floor"** of protections, they are **not even** to serve as a **"best practices"** standard;

2. The HIPAA Privacy Rule still **"permits"** covered entities – providers and health plans to obtain consent; (need to give examples of who's left out)

3. **More stringent (protective) state laws** (such as those mentioned above) are not weakened or preempted; and

4. **Ethical standards** retain "their vitality". [22]

D. **Other problems magnified** by the Rule

i. Privacy protections apply **only to** covered entities which include **only** providers, health plans and healthcare clearinghouses and not others who handle health information;

ii. **No notice** requirement for privacy breaches;

iii. **No accounting** for routine disclosures;

iv. **Weak enforcement** provisions—over 17,000 complaints of privacy violations but only one enforcement action since April 14, 2003. [23]

v. No **private right of action.**

---

[22] 67 Fed. Reg. at 53,212 Tab 3.
[23] Office of Civil Rights quoted in Reading Eagle (Feb. 24, 2006)

VI. What does the public expect and want?

A. HHS—Public has a **"common belief"** and **"strong expectation"** that their identifiable health information will not be disclosed without their consent. [24]

B. Supreme Court—Patients have a **"reasonable expectation"** that diagnostic tests will not be shared with non-medical personnel without their consent. [25]

C. **65% of Americans** would not disclose sensitive but necessary information to their physicians and providers if they thought it would go into an electronic health information system. [26]

D. **75% of Americans** are concerned about the loss of medical privacy due to the use of an electronic health information system. [27]

E. **63% of Americans** would not take a genetic test if the results were communicated to their insurers or employers, [28]

F. **35% of people** offered a free genetic test to access the risk of breast cancer declined citing loss of privacy concerns. [29]

G. **Adverse effects** of privacy concerns on patients:
   i. approximately **600,000 people** annually do not seek early diagnosis and treatment for cancer,

---

[24] 65 Fed. Reg. at 82,472.
[25] Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).
[26] Report of study by Center for Social and Legal Research presented to the National Committee on Vital and Health Statistics, by Dr. Alan Westin, Professor of Public Law & Government, Columbia University (February 23, 2005).
[27] Ethics Survey of Consumer Attitudes about Health Web Sites, California Health Care Foundation , at 3 (January 2000).
[28] 65 Fed. Reg. at 82,466.
[29] Id.

ii. more than **2 million people** annually do not seek needed treatment for mental illness,

iii. **many people** do not seek treatment for sexually transmitted diseases, [30]

iv. "**one in six Americans** take evasive action to avoid privacy violations including providing inaccurate information, changing physicians, or avoiding health care altogether." [31]

v. **87% of physicians** report withholding information from a patient's medical record due to privacy concerns. [32]

VII. A health IT system poses a greater threat to health privacy.

A. HHS—"In a matter of seconds, a person's most profoundly private information can be shared with **hundreds, thousands, even millions of individuals and organizations at a time....**[eliminating] many of the financial and logistical obstacles that previously served to protect the confidentiality of health information and the privacy interests of individuals." [33]

B. Health IT creates the potential for breaches of health information privacy on **a scale previously unimaginable.**[34]

C. Once health information is disclosed electronically, it **cannot be recovered.**

---

[30] 65 Fed. Reg. at 82,778.
[31] 65 Fed. Reg. at 82,468.
[32] Id.
[33] 65 Fed. Reg. at 82,465.
[34] "Theft Nabs Backup Data on 365,000 Patients", Computerworld (January 26, 2006)

D. HHS—"there is **no such thing** as a totally secure [electronic information] system that carries no risk". [35]

E. Findings of the **President's Information Technology Advisory Committee:**

i. the nation's electronic information systems are **"highly vulnerable"** to corruption by hackers and others;

ii. "the threat is clearly growing" with attacks rising by **"over 20 percent annually"**;

iii. the increasing **vulnerabilities cannot be addressed** by the current "patching" approach, and new research is needed "to design security into computing and networking systems and software from the ground up." [36]

VIII. Concerns with H.R. 4157 – Overall – patients want meaningful control and adequate enforcement. This bill does not accomplish either.

A. It authorizes the Secretary to issue a **"single set of national standards"** for the privacy of health information.

B. And it allows the Secretary to **preempt privacy protections in State laws** "to the extent **the Secretary determines**" such standards are "necessary to promote uniformity and efficiency". Section 4(b)(1). The study fails to assess existing national privacy standards and why certain state laws are in place and what value they have for patients.

C. **Given Congress' past inability** to reach agreement on key issues, the process is virtually guaranteed to result in

---

[35] 68 Fed. Reg.at 8,346.

[36] "Cyber Security: A Crisis in Prioritization", President's Information Technology Advisory Committee, at 7-12 (February 23, 2005).

the Secretary of HHS setting the national privacy standard.

D. **Unelected government officials**, such as the Secretary of HHS, should not be given **the power to eliminate "fundamental and cherished" rights** of citizens.

IX. The right course of action for Congress

A. Ground any health IT system in the **strong privacy standards reflected in the history of the nation** in professional and medical ethics, the law of medical and psychotherapy privilege, federal and state law, and constitutional common law.

B. Provide for **meaningful, informed patient consent** which allows patients some control over whether their health information is shared over a national health network and what information may be shared.

C. **Bring the "floor" of privacy protections in the HIPAA Privacy Rule** into conformity with existing national privacy standards and citizens' expectations.

D. Provide health information privacy protections that apply **to anyone** who handles the information.

E. Provide for **prompt notification** of the individual and the Secretary of any actual or suspected privacy breach and require the Secretary to maintain a **publicly accessible list** of organizations that have had privacy breaches and the remedial action taken.

F. Require an **electronic audit trail** for the disclosure of all health information.

G. Provide for **electronic segregation** of highly sensitive health information into more secure electronic sites.

H. Provide for individuals to be able **to opt in or opt out** of such systems fully or with respect to certain information.

I. Provide strong protections to prevent **employers** from gaining access to their employees' health information.

J. Provide for a **private right of action** to obtain injunctive relief and damages for privacy breaches.

X. Finally, there is the **Bartnicki** problem.

A. According to the Supreme Court, the media has a First Amendment **right to publish** information about any matter of "public or general interest" **even if that information is obtained unlawfully**. Bartnicki v. Vopper, 532 U.S. 514, 534 (2001).

B. Thus, any health information obtained by someone hacking into an electronic health information system could be **published on the front page of the Washington Post** if it concerned a public official.

C. This could include **any member of the Administration or Congress**, members of state administrations and legislatures, state and local boards, officials of political parties.

D. Congress **could not pass a law** to prevent that publication.

E. Under an electronic health information system with the HIPAA privacy protections, it is **unlikely that Presidents Kennedy or Reagan would have ever reached the White House.**

F. Unless the strongest possible privacy protections are included in any health IT bill, **federal and state elections** in the future will be determined by the content of the candidates' medical records.

James C. Pyles
Powers, Pyles, Sutter and Verville, P.C.
1875 Eye Street, 12th Floor
Washington, D.C. 20006
(202) 466-6550
jim.pyles@ppsv.com

On behalf of the American Psychoanalytic Association

FINDINGS AND FACTS IN SUPPORT OF ETHICS BASED MEDICAL PRIVACY

(1) **The entire health delivery system** is based upon the willingness of the individual to trust a health care practitioner sufficiently to disclose to the practitioner the most intimate details of his or her life.[1]

(2) An assurance of **privacy** of health information is **necessary to secure effective, high quality health care.**[2]

(3) The "**reason and experience**" of the country shows that effective psychotherapy is dependent an atmosphere of trust confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories and fears without fear of nonconsensual uses and disclosures.[3]

(4) Adequate protection of the **security and privacy** of health information is a ***sine qua non* of the increased efficiency of information exchange brought about by the electronic revolution.**[4]

(5) Citizens have a **reasonable expectation** that their most intimate identifiable health information will not be used and disclosed in routine situations without their consent or over their objections.[5]

(6) The public is **increasingly concerned** about the loss of personal privacy due to the increasing use of **interconnected electronic information systems** which make it possible in a matter of seconds to share a person's most profoundly private information with hundreds, thousands, and even millions of individuals and organizations.[6]

(7) A recent study found that **70% of the public is concerned that their health information will be leaked or shared without their**

---

[1] See 65 Fed. Reg. at 82,467, finding of the U.S. Department of Health and Human Services in issuing the Original Standards for Privacy of Individually Identifiable Health Information after one of the most extensive rulemaking proceedings in the history of the department. This HHS finding, as well as those listed below, were confirmed by HHS when the Original Privacy Rule was put into effect without change by the current Administration (66 Fed. Reg. at 12,434). None of these findings was retracted when the Original Rule was amended on August 14, 2002 (67 Fed. Reg. 53,182).

[2] 65 Fed. Reg. at 82,467.

[3] Jaffee v. Redmond, 116 S. Ct. 1923, 1928 (1996).

[4] 65 Fed. Reg. at 82,474.

[5] Ferguson v. City of Charleston, 121 S. Ct. 1281, 1288 (2001); Statement of Massachusetts Medical Society, "Patient Privacy and Confidentiality" (1996); finding by HHS (65 Fed. Reg. at 82,472).

[6] 65 Fed. Reg. at 82,465.

permission by an electronic health information system.[7] It also found that **65% of Americans would not disclose sensitive but necessary health information to doctors and health care providers** because of worries that the information will go into an electronic health information system.[8] This is consistent with HHS' earlier findings that annually **600,000 citizens** do not seek early diagnosis and treatment for cancer, **2 million citizens** do not seek treatment for mental illness and **thousands of citizens** do not seek treatment for sexually transmitted diseases due to privacy concerns. [9]

(8) The privacy of identifiable health information depends in large part on the existence of security measures to prevent unwanted disclosures. However, **there is no such thing as a totally secure electronic information system.**[10]

(9) The nation's electronic information systems are **highly vulnerable** to unauthorized intrusion, the attacks and **vulnerabilities are growing** rapidly, and they cannot be addressed adequately with current technology.[11]

10) Federal agencies have taken **even fewer measures** than the private sector to identify and address the growing threats to cyber security.[12]

11) Privacy is a **fundamental right**.[13]

12) **All fifty states** today recognize in tort law a common law or statutory right to privacy. Some states, such as Tennessee and California, have a right to privacy as a matter of **state constitutional law**.[14]

13)Many of the most basic protections in the Constitution of the United States are imbued with an attempt to protect individual privacy while balancing it against larger societal purposes of the nation. The right to privacy is reflected in the **First Amendment's** protection of freedom of religion, the **Second Amendment's** protection of the right to keep and bear arms, the **Third Amendment's** protection of the right to not have

---

[7] Testimony of Dr. Alan F. Westin, Professor of Public Law & Government Emeritus, Columbia University at Hearing on Privacy and Health Information Technology before the NCVHS Subcommittee on Privacy, at 5, (February 23, 2005).
[8] Id.
[9] 65 Fed. Reg. at 82,778.
[10] 68 Fed. Reg. at 8,335, 8,346.
[11] "Cyber Security: A Crisis of Prioritization: Report to the President", President's Information Technology Advisory Committee, 5-12 (February 28, 2005).
[12] "Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems", General Accountability Office, GAO-05-231, at 6 (May 13, 2005).
[13] 65 Fed. Reg. at 82,464 (December 28, 2000).
[14] Id.

soldiers quartered in one's house without consent, the **Fourth Amendment's** protection against unreasonable searches and seizures, the **Fifth and Fourteenth Amendments'** protection of the right to Liberty, and the **Ninth Amendment's** protection of rights retained by the people.[15]

14) The **right to privacy** is "the claim of individuals, groups, or institutions to determine for themselves, **when, how, and to what extent** information about them is communicated."[16]

15) **The Hippocratic Oath**, since the 5th century B.C., has recognized that physicians have a duty to keep patient information confidential. The Oath has remained in Western Civilization as an expression of ideal conduct for the physician.[17] The Oath is administered to the graduates of 98% of the medical schools in the United States and Canada.[18]

16) **Current standards of medical ethics** of virtually every segment of the medical profession provide that identifiable health information should not be disclosed without the patient's informed consent:

a. **The American Medical Association**: "A physician shall...safeguard patient confidences within the constraints of the law."

"The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law."[19]

b. **The American College of Physicians—American Society of Internal Medicine**: "Confidentiality is a fundamental tenet of medical care...The physician must not release information without the patient's consent (often termed a 'privileged communication')."[20]

c. **The Association of American Physicians and Surgeons**: "The special importance of the patient's privacy in medical matters requires that the physician never reveal either the confidence entrusted to him in the course of medical

---

[15] Id.
[16] A. Cavoukian, D. Tapscott, "Who Knows: Safeguarding Your Privacy in a Networked World," Random House (1995).
[17] American Medical Association, Code of Medical Ethics, History (2001).
[18] R. Orr, M.D., and N. Pang, M.D., The Use of the Hippocratic Oath: A Review of 20th Century Practice and a Content Analysis of Oaths Administered in Medical Schools in the U.S. and Canada in 1993.
[19] American Medical Association, Principles of Medical Ethics, IV; Current Opinions of the Council on Ethical and Judicial Affairs, E-5.05 (1998).
[20] American College of Physicians—American Society of Internal Medicine, Ethics Manual (1998).

attendance, or deficiencies he may observe in the character of the patient, releasing information only with the consent of the patient and with due consideration of the mandates of law.[21]

d. **The American Dental Association**: "The dentist has a duty to respect the patient's rights to self-determination and confidentiality."

   "Dentists are obligated to safeguard the confidentiality of patient records."[22]

e. **The American Academy of Physical Medicine and Rehabilitation**: "Patient confidentiality must be respected at all times. This includes confidentiality of the medical records. Patient's privacy should be honored unless mandated by law. Consent of the patient or other responsible party should be obtained for release of information."[23]

f. **The American Nursing Association**: "The nurse safeguards the patient's right to privacy. The need for health care does not justify unwanted intrusion into a patient's life. The nurse advocates for an environment that provides for sufficient physical privacy, including auditory privacy for discussions of a personal nature and policies and practices that protect the confidentiality of information.

   Associated with the right to privacy, the nurse has a duty to maintain confidentiality of all patient information. The patient's well-being could be jeopardized and the fundamental trust between the patient and the nurse destroyed by unnecessary access to data or by the inappropriate disclosure of identifiable patient information."[24]

g. **The American Psychiatric Association**: "A physician shall respect the rights of patients, colleagues, and other health professionals, and shall safeguard patient confidences and privacy within the constraints of the law. Psychiatric records, including even the identification of a person as a patient, must be protected with extreme care.

---

[21] Association of American Physicians and Surgeons, Principles of Medical Ethics, (9) (January 1991).
[22] American Dental Association, Principles, Code of Professional Conduct and Advisory Opinions, Section 1.
[23] American Academy of Physical Medicine and Rehabilitation, Code of Conduct, II. Ethics Relating to the Patient and the Patient's Family.
[24] American Nursing Association, Code of Ethics, 3.1, 3.2.

Confidentiality is essential to psychiatric treatment. This is based in part on the special nature of psychiatric therapy as well as on the traditional ethical relationship between physician and patient. Growing concern regarding the civil rights of patients and the possible adverse effects of computerization, duplication equipment, and data banks makes the dissemination of confidential information an increasing hazard....

A psychiatrist may release confidential information only with the authorization of the patient or under proper legal compulsion."[25]

h. **The American Psychoanalytic Association**: "Confidentiality of the patient's communications is a basic patient's right and an essential condition for effective psychoanalytic treatment and research...

All information about the specifics of a patient's life is confidential, including the name of the patient and the fact of treatment. The psychoanalyst should resist disclosing confidential information to the full extent permitted by law....

The psychoanalyst should never share confidential information about a patient with nonclinical third-parties (e.g. insurance companies) without the patient's or, in the case of a minor patient, the patient's or guardian's informed consent."[26]

i. **The American Psychological Association**: "Psychologists have a primary obligation and take reasonable precautions to protect confidential information obtained through or stored in any medium, recognizing that the extent and limits of confidentiality may be regulated by law or established by institutional rules or professional or scientific relationship....

Psychologists may disclose confidential information with the appropriate consent of the organizational client, the individual client/patient, or another legally authorized person on behalf of the client/patient unless prohibited by law.

Psychologists disclose confidential information without the consent of the individual only as mandated by law, or where permitted by law for a valid purpose such as to (1) provide needed professional services; (2) obtain appropriate

---

[25] American Psychiatric Association, Principles of Medical Ethics with Annotations Especially Applicable to Psychiatry, Section 4 (2001).

[26] American Psychoanalytic Association, Principles and Standards of Ethics for Psychoanalysts, General Guiding Principles, IV., Standards Applicable to the Principles of Ethics for Psychoanalysts, IV.2.

professional consultations; (3) protect the client/patient, psychologist, or others from harm; or (4) obtain payment for services from a client/patient, in which instance disclosure is limited to the minimum that is necessary to achieve the purpose."[27]

j. **The National Association of Social Workers**: "Social workers should respect clients' right to privacy. Social workers should not solicit private information from clients unless it is essential to providing services or conducting social work evaluation or research. Once private information is shared, standards of confidentiality apply....

Social workers may disclose confidential information when appropriate with valid consent from a client or a person legally authorized to consent on behalf of a client.[28]

k. **Clinical Social Work Federation**: "Clinical social workers have a primary obligation to maintain the privacy of both current and former clients, whether living or deceased, and to maintain the confidentiality of material that has been transmitted to them in any of their professional roles. Exceptions to this responsibility will occur only where there are overriding legal or professional reasons and, whenever possible, with the written and informed consent of the client(s)."[29]

l. **American College of Emergency Room Physicians**: "The principles listed below express fundamental moral responsibilities of emergency physicians....

Emergency physicians shall...Respect patient privacy and disclose confidential information only with consent of the patient or when required by an overriding duty such as the duty to protect others or to obey the law."[30]

m. **American Physical Therapy Association**: "Information relating to the physical therapist/patient relationship is confidential and may not be communicated to a third party not involved in that

---

[27] American Psychological Association, Ethical Principles of Psychologists and Code of Conduct, Ethical Standards, Maintaining Confidentiality, 4.01, Disclosures, 4.05 (June 1, 2003).
[28] National Association of Social Workers, Ethical Standards, 1.07 Privacy and Confidentiality (1999).
[29] Clinical Social Work Federation, Code of Ethics, III. Confidentiality (2003).
[30] American College of Emergency Room Physicians, Code of Ethics, Principles of Ethics for Emergency Physicians, 5 (October 2001).

patient's care without the prior consent of the patient, subject to applicable law."[31]

n. **American Society of Radiologic Technologists**: "The radiologic technologist respects confidences entrusted in the course of professional practice, respects the patient's right to privacy and reveals confidential information only as required by law or to protect the welfare of the individual or the community.[32]

o. **American Pharmacy Association**: "This Code, prepared and supported by pharmacists, is intended to state publicly the principles that form the fundamental basis of the roles and responsibilities of pharmacists. These principles, based on moral obligations and virtues, are established to guide pharmacists in relationships with patients, health professionals, and society.[33]

A pharmacist is dedicated to protecting the dignity of the patient. With a caring attitude and a compassionate spirit, a pharmacist focuses on serving the patient in a private and confidential manner.

p. **National Community Pharmacists Association**: "NCPA strenuously opposes electronic prescription transmission programs or manufacturers' marketing program, such as patient information or poverty relief, that violate the integrity and confidentiality of the face-to-face relationship between the patient and the community pharmacist. NCPA supports explicit patient medical releases that prevent patient-specific data from being extracted, provided, or sold to extraneous parties without the informed and express written consent of the patient.[34]

17) Standards of medical ethics define **moral principles** for the practice of medicine. **Unethical conduct** in the practice of medicine is professional conduct that fails to conform to these moral standards or policies.[35]

18) As a matter of medical ethics and constitutional principles deeply rooted in the nation's history and tradition, law abiding citizens who

---

[31] American Physical Therapy Association, APTA Guide for Professional Conduct, Ethical Principle, 2.3 Confidential Information (January 2004).
[32] American Society of Radiologic Technologists and the American Registry of Radiologic Technologists, Code of Ethics, (9) (February 2003).
[33] American Pharmacy Association, Code of Ethics for Pharmacists, Preamble and Section II.
[34] National Community Pharmacists Association, Patient Confidentiality/Privacy, Position Statement.
[35] American Medical Association, Current Opinions of the Council on Ethics and Judicial Affairs, E-1.01 Terminology (June 1996).

pose no health threat to society should not have their intimate health information used or disclosed without notice, without their consent or over their objection and should not be compelled or coerced to disclose their identifiable health information to an electronic health information system that cannot guarantee the privacy of that information.

Georgia Health Information Privacy Laws

1. HMOs

HMOs may not disclose any information pertaining to diagnosis, treatment or health of any enrollee or applicant or information from any provider without the patient's or applicant's express consent. Ga. Code Ann. 33-21-23.

2. Physicians, hospitals, health care facilities and pharmacies

Physicians, hospitals, health care facilities and pharmacists generally may not be required to release any medical information concerning a patient accept upon written authorization. Ga. Code Ann. 24-9-40.

3. Insurance entities

Generally, an insurance entity may not disclose medical information about a person it collected or received in connection with an insurance transaction without that person's written authorization. Ga. Code Ann. 33-39-14.

4. Residents of long term care facilities

Residents of long term care facilities have a right to privacy in their medical, personal and bodily care programs. Case discussions, consultations, examinations, treatments, and care are confidential and are to be conducted in privacy. Ga. Code Ann. 31-8-114(6).

5. Genetic testing

Information derived from genetic testing is confidential and may be released only to the individual tested and to persons specifically authorized by such individual in writing. Ga. Code Ann. 33-54-3.

6. HIV/AIDS

A person or entity that is responsible for recording, reporting, or maintaining AIDS confidential information or that receives that information as permitted by law may not intentionally or knowingly disclose that information to another. Ga. Code Ann. 24-9-47(b).

7. **Mental health records**

Mental health records may not be released except with patient authorization and in several other limited circumstances. Ga. Code Ann. 37-3-166.

8. **Privileges**

Psychotherapy communications and information are subject to a psychotherapist-patient privilege which applies to patients of psychiatrists, licensed psychologists, licensed clinical social workers, licensed marriage counselors and others who render psychotherapy. Ga. Code Ann. 24-9-21.

9. **Private right of action**

A private right of action is available for privacy violations by insurance companies and HMOs [Ga. Code Ann. 33-39-22] and for the improper disclosure of genetic testing information [Ga. Code Ann. 33-54-8].

Ohio Health Information Privacy Laws

1. Health Insuring Corporation

Health information pertaining to an individual's treatment or health obtained by a health insuring corporation from the individual or any health care facility must be held in confidence and may not be disclosed without the express consent of the individual, with several limited exceptions. Oh. Rev. Code 1751.52.

2. Insurance entities including health insuring corporations

Generally, an insurance entity may not disclose medical information about a person that it collected or received in connection with an insurance transaction without that person's written authorization. Oh. Rev. Code 3904.13.

3. Nursing home residents

Nursing home residents have a right to confidential treatment of personal and medical records, and the right to approve or refuse the release of their records to any individual outside the home, with limited exceptions. Oh. Rev. Code 3721.13.

4. Physicians, physicians assistants and psychologists

Physicians and physicians' assistants who betray a professional confidence can be brought before the State Medical Board for disciplinary action. Oh. Rev. Code 4730.25(B)(7); 4731.22(B)(4). The same is true for psychologists who make unauthorized disclosures of information received in confidence. Oh. Rev. Code 4732.17.

5. Birth defects

Records and information concerning birth defects are confidential and may not be disclosed without the written

consent of the child's parent or legal guardian, with limited exceptions. Oh. Rev. Code 3705.32.

6. Genetic test results

Insurers and health insuring corporations may not require, consider, or inquire into the results of genetic screening or testing in processing an application for insurance coverage. Oh. Rev. Code 1751.64; 3901.49; 3901.50.

7. HIV/AIDS

No person who acquires HIV-related information while providing any health care service or while employed by a health care provider or facility may disclose the identity of any individual on whom an HIV test is performed, the results of the test, or the identity of any person diagnosed as having AIDS or an AIDS related condition without the written authorization of the individual. Oh. Rev. Code 3701.243(A).

8. Privileges

Ohio recognizes a privilege protecting communications between patients and physicians, dentists, chiropractors, school guidance counselors, professional counselors and social workers and psychologists. Oh. Rev. Code 2317.02(B)(1), 2317.02(J)(1), 2317.02(G)(1), and 4732.19.

9. Private right of action

A private right of action exists for unauthorized disclosures of health information by insurers and health insuring corporations [Oh. Rev. Code 3904.2] and for the unauthorized disclosure of HIV/AIDS information [Oh. Rev. Code 3701.244].

The Department adopts the approach that was proposed in the NPRM, because it is the only one that resolves the operational problems that have been identified in a simple and uniform manner. First, this Rule strengthens the notice requirements to preserve the opportunity for individuals to discuss privacy practices and concerns with providers. (See section III.H. of the preamble for the related discussion of modifications to strengthen the notice requirements.) Second, the final Rule makes the obtaining of consent to use and disclose protected health information for treatment, payment, or health care operations optional on the part of all covered entities, including providers with direct treatment relationships. A health care provider that has a direct treatment relationship with an individual is not required by the Privacy Rule to obtain an individual's consent prior to using and disclosing information about him or her for treatment, payment, and health care operations. They, like other covered entities, have regulatory permission for such uses and disclosures. The fact that there is a State law that has been using a similar model for years provides us confidence that this is a workable approach.

Other rights provided by the Rule are not affected by this modification. Although covered entities will not be required to obtain an individual's consent, any uses or disclosures of protected health information for treatment, payment, or health care operations must still be consistent with the covered entity's notice of privacy practices. Also, the removal of the consent requirement applies only to consent for treatment, payment, and health care operations; it does not alter the requirement to obtain an authorization under § 164.508 for uses and disclosures of protected health information not otherwise permitted by the Privacy Rule or any other requirements for the use or disclosure of protected health information. The Department intends to enforce strictly the requirement for obtaining an individual's authorization, in accordance with § 164.508, for uses and disclosure of protected health information for purposes not otherwise permitted or required by the Privacy Rule. Furthermore, individuals retain the right to request restrictions, in accordance with § 164.522(a). This allows individuals and covered entities to enter into agreements to restrict uses and disclosures of protected health information for treatment, payment, and health care operations that are enforceable under the Privacy Rule.

Although consent for use and disclosure of protected health information for treatment, payment, and health care operations is no longer mandated, this Final Rule allows covered entities to have a consent process if they wish to do so. The Department heard from many commenters that obtaining consent was an integral part of the ethical and other practice standards for many health care professionals. It, therefore, does not prohibit covered entities from obtaining consent.

This final Rule allows covered entities that choose to have a consent process complete discretion in designing that process. Prior comments have informed the Department that one consent process and one set of principles will likely be unworkable. Covered entities that choose to obtain consent may rely on industry practices to design a voluntary consent process that works best for their practice area and consumers, but they are not required to do so.

This final Rule effectuates these changes in the same manner as proposed by the NPRM. The consent provisions in § 164.506 are replaced with a new provision at § 164.506(a) that provides regulatory permission for covered entities to use or disclose protected health information for treatment, payment, and health care operations. A new provision is added at § 164.506(b) that permits covered entities to obtain consent if they choose to, and makes clear any such consent process does not override or alter the authorization requirements in § 164.508. Section 164.506(b) includes a small change from the proposed version to make it clearer that authorizations are still required by referring directly to authorizations under § 164.508.

Additionally, this final Rule includes a number of conforming modifications, identical to those proposed in the NPRM, to accommodate the new approach. The most substantive corresponding changes are at §§ 164.502 and 164.532. Section 164.502(a)(1) provides a list of the permissible uses and disclosures of protected health information, and refers to the corresponding section of the Privacy Rule for the detailed requirements. The provisions at §§ 164.502(a)(1)(ii) and (iii) that address uses and disclosures of protected health information for treatment, payment, and health care operations are collapsed into a single provision, and the language is modified to eliminate the consent requirement.

The references in § 164.532 to § 164.506 and to consent, authorization, or other express legal permission obtained for uses and disclosures of protected health information for treatment, payment, and health care operations prior to the compliance date of the Privacy Rule are deleted. The proposal to permit a covered entity to use or disclose protected health information for these purposes without consent or authorization would apply to any protected health information held by a covered entity whether created or received before or after the compliance date. Therefore, transition provisions are not necessary.

This final Rule also includes conforming changes to the definition of "more stringent" in § 160.202; the text of § 164.500(b)(1)(v), §§ 164.508(a)(2)(i) and (b)(3)(i), and § 164.520(b)(1)(ii)(B); the introductory text of §§ 164.510 and 164.512, and the title of § 164.512 to eliminate references to required consent.

Response to Other Public Comments

Comment: There were three categories of commenters with respect to the Rule's general approach to consent-those that supported the changes proposed in the NPRM provisions, those that requested targeted changes to the consent requirement, and those that requested that the consent requirement be strengthened.

Many commenters supported the NPRM approach to consent, making consent to use or disclose protected health information for treatment, payment, and health care operations voluntary for all covered entities. These commenters said that this approach provided flexibility for covered entities to address consent in a way that is consistent with their practices. These commenters also stated that the NPRM approach assured that the Privacy Rule would not interfere with or delay necessary treatment.

Those that advocated retaining a consent requirement stated that the NPRM approach would undermine trust in the health care system and that requiring consent before using or disclosing protected health information shows respect for the patient's autonomy, underscores the need to inform the patient of the risks and benefits of sharing protected health information, and makes it possible for the patient to make an informed decision. Many of these commenters suggested that the consent requirement be retained and that the problems raised by consent be addressed through targeted changes or guidance for each issue.

Some suggestions targeted to specific problems were: (1) Fix the problems

(3) That designates health care components in accordance with paragraph (c)(3)(iii) of this section.

* * * * *

(c)(1) *Implementation specification: Application of other provisions.* * * *

(ii) A reference in such provision to a "health plan," "covered health care provider," or "health care clearinghouse" refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable; and

* * * * *

(2) *Implementation specifications: Safeguard requirements.* * * *

(ii) A component that is described by paragraph (c)(3)(iii)(B) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by this subpart; and

* * * * *

(3) *Implementation specifications: Responsibilities of the covered entity.*

* * *

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j), provided that, if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs:

(A) Covered functions; or

(B) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

* * * * *

(f)(1) *Standard: Requirements for group health plans.* (i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

* * * * *

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

* * * * *

7. Revise § 164.506 to read as follows:

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) *Standard: Consent for uses and disclosures permitted.* (1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.*

(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

8. Revise § 164.508 to read as follows:

§ 164.508 Uses and disclosures for which an authorization is required.

(a) *Standard: authorizations for uses and disclosures.*—(1) *Authorization required: general rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) *Authorization required: psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) *Authorization required: Marketing.* (i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health

related to filling prescriptions by treating pharmacists as providers with indirect treatment relationships or by deeming a prescription to serve as an implied consent; and (2) allow certain uses and disclosures prior to first patient encounter. Some of these commenters argued that certain issues could be addressed through guidance on other provisions in the Rule, rather than a change in the regulation. For example, they suggested that guidance could explain that physicians who take phone calls for one another are part of an organized health care arrangement, or could provide technical assistance about revocations on consent by identifying when a covered entity has taken action in reliance on a consent.

Other suggestions were more general. They included suggestions that the Department: (1) Substitute a good faith effort requirement for the current provisions; (2) provide regulatory permission for certain uses and disclosures of protected heath information prior to first service delivery; (3) permit oral consent with documentation; (4) retain a consent requirement for disclosures, but not uses; (5) retain a consent requirement for payment and operations, but not treatment uses and disclosures; (6) allow individuals to opt out of the consent requirement; (7) allow the consent to apply to activities of referred-to providers, and (8) retain the consent requirement but add flexibility, not exceptions.

The third group of commenters requested that the consent requirement be strengthened. Some requested that the Privacy Rule not permit conditioning of treatment or enrollment on consent for multiple uses and disclosures. Others requested that the consent requirement be extended to covered entities other than providers with direct treatment relationships, such as health plans. Some commenters also asked that the consent be time-limited or be required more frequently, such as at each service delivery.

Response: The Department recognizes that there are some benefits to the consent requirement and has considered all options to preserve the consent requirement while fixing the problems it raises. After examining each of these options, we do not believe that any would address all of the issues that were brought to the Department's attention during the comment process or would be the best approach for regulating this area. For example, the suggestion to treat pharmacists as indirect treatment providers would not be consistent with the current regulatory definition of that term and would not have addressed other referral situations. This approach was also rejected by some pharmacists who view themselves as providing treatment directly to individuals. The suggestion to allow certain uses and disclosures prior to first patient encounter would not address concerns of tracking consents, use of historical data for quality purposes, or the concerns of emergency treatment providers.

The Department desired a global approach to resolving the problems raised by the prior consent requirement, so as not to add additional complexity to the Privacy Rule or apply different standards to different types of direct treatment providers. This approach is consistent with the basic goal of the Rule to provide flexibility as necessary for the standards to work for all sectors of the health care industry.

More global approaches suggested were carefully considered, but each had some flaw or failed to address all of the treatment-related concerns brought to our attention. For example, those who suggested that the Rule be modified to require a good faith effort to obtain consent at first service delivery failed to explain how that approach would provide additional protection than the approach we proposed. The Department also decided against eliminating the consent requirement only for uses and disclosures for treatment, or only for uses of protected health information but not for disclosures, because these options fall short of addressing all of the problems raised. Scheduling appointments and surgeries, and conducting many pre-admission activities, are health care operations activities, not treatment. Retaining the consent requirement for payment would be problematic because, in cases where a provider, such as a pharmacist or hospital, engages in a payment activity prior to face-to-face contact with the individual, it would prohibit the provider from contacting insurance companies to obtain pre-certification or to verify coverage.

Similarly, the suggestion to limit the prior consent requirement to disclosures and not to uses would not have addressed all of the problems raised by the consent requirements. Many of the basic activities that occur before the initial face-to-face meeting between a provider and an individual involve disclosures as well as uses. Like the previous approach, this approach also would prohibit pharmacists and hospitals from contacting insurance companies to obtain pre-certification or verify coverage if they did not have the individual's prior consent to disclose the protected health information for payment. It also would prohibit a provider from contacting another provider to ask questions about the medical record and discuss the patient's condition, because this would be a disclosure and would require consent.

There was a substantial amount of support from commenters for the approach taken in the NPRM. The Department continues to believe that this approach makes the most sense and meets the goals of not interfering with access to quality health care and of providing a single standard that works for the entire health care industry. Therefore, the Department has adopted the approach proposed in the NPRM.

Comment: Some commenters asserted that eliminating the consent requirement would be a departure from current medical ethical standards that protect patient confidentiality and common law and State law remedies for breach of confidentiality that generally require or support patient consent prior to disclosing patient information for any reason. Another commenter was concerned that the removal of the consent requirement from the Privacy Rule will become the de facto industry standard and supplant professional ethical duties to obtain consent for the use of protected health information.

Response: The Privacy Rule provides a floor of privacy protection. State laws that are more stringent remain in force. In order not to interfere with such laws and ethical standards, this Rule permits covered entities to obtain consent. Nor is the Privacy Rule intended to serve as a "best practices" standard. Thus, professional standards that are more protective of privacy retain their vitality.

Comment: Some commenters requested that, if the Department adopts the NPRM approach to eliminate the consent requirement for uses and disclosures of protected health information for treatment, payment, or health care operations, the definition of "health care operations" should also be narrowed to protect individual expectations of privacy.

Response: We disagree. As stated in the preamble to the December 2000 Privacy Rule, the Department believes that narrowing the definition of "health care operations" will place serious burdens on covered entities and impair their ability to conduct legitimate business and management functions.

Comment: Some commenters requested that the regulation text state more specifically that a voluntary consent cannot substitute for an authorization when an authorization is otherwise required under the Privacy Rule.

TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS
45 C.F.R. 164.501

"Treatment"

1. provision of health care
2. management of health care
3. coordination of health care
4. management of health care
5. consultation between health care providers relating to a patient
6. the referral of a patient for health care from one provider to another. 45 CFR 164.501

"Payment"

Activities by a health plan or a provider with respect to providing or obtaining reimbursement for services "including, but not limited to"

1. determinations of eligibility
2. determinations of coverage
3. adjudications of health claims
4. subrogation of health claims
5. risking adjusting amounts due based on enrollee status and demographic characteristics
6. billing
7. claims management
8. collection activities
9. obtaining payment under a contract for reinsurance
10. related health care data processing
11. review of health services with respect to medical necessity
12. review of health services with respect to coverage under a health plan
13. review of health services with respect to appropriateness of care
14. review of health services with respect to justification of charges
15. utilization review activities
16. concurrent review of services
17. retrospective review of services
18. disclosure to consumer reporting agencies

"Health Care Operations"

1. conducting quality assessment and improvement activities
2. development of clinical guidelines
3. population based activities related to improving health
4. population based activities related to reducing health care costs
5. population based activities related to protocol development
6. population based activities related to case management and care coordination
7. contacting of health care providers with information about treatment alternatives
8. contacting of patients with information about treatment alternatives
9. related functions that do not include treatment
10. reviewing the competence of health care professionals
11. reviewing the qualifications of health care professionals
12. evaluating practitioner performance
13. evaluating provider performance
14. evaluating health plan performance
15. conducting training programs for students, trainees or practitioners
16. training of non-health care professionals
17. accreditation
18. certification
19. licensing
20. credentialing activities
21. underwriting
22. premium rating
23. other activities relating to the creation, renewal or replacement of a contract of health insurance
24. ceding a contract for reinsurance
25. securing a contract for reinsurance
26. placing a contract for reinsurance
27. conducting or arranging medical review
28. conducting or arranging legal services
29. conducting or arranging auditing functions
30. conducting or arranging for fraud and abuse detection programs
31. conducting or arranging for compliance programs
32. business planning
33. business development
34. business management
35. general administrative activities of the entity
36. customer service including provision of data analysis for policy
37. resolution of internal grievances
38. sale of the covered entity
39. transfer of the covered entity
40. merger of the covered entity
41. consolidation of the covered entity
42. due diligence pertaining to items 38-41
43. creating de-identified health information
44. creating a limited data set
45. fundraising

"Treatment and payment" uses relate to providing health care to the individual while **"health care operations"** uses relate to operations of the covered entity. 65 Fed. Reg. at 82,489/3, 82,495/1, 82,4973.